Security Policy for IC3500

BT-140722-042-PCI-001

Document version: 1.4

Version History

Revision	Date	Editor	Description
1.0	July.02.2014	YJ Kim	Initial release
1.1	July.23.2014	YJ Kim	Added some more chapter
1.2	Aug.11.2014	YJ Kim	Added software update and patch procedure.
1.3	Aug.18.2014	YJ Kim	Added Key managements
1.4	Aug.20.2014	YJ Kim	Add to Visual Shield Installation Guidance.

Contents

1. Introduction

This document addresses the proper use of the POI in a secure fashion, including information about key-management responsibilities, device functionality, identification, environmental requirements and administrative responsibilities. Also this document including installation with operation guidance to use of IC3500 model

1.1 Glossary

AES	Advanced Encryption Standard
RSA	Rivest Shamir Adelman Algorithm
SHA	secure Hash Algorithm
TDES	Triple Data Encryption Standard
PIN	Personal Identification Number
DUKPT	Derived unique Key per Transaction

2. General description

This Document is to provide indication to answer the security requirements as listed in DTR B20 in the PCI PTS POI Version 4.0

2.1 Product overview

The IC3500 is designed as desktop POS device to support PIN entry with credit and debit based transaction in attended environment. This device has TFT color LCD with Touch screen for operation. Also this device Provide ICCR, MSR, thermal printer, USB port, micro-USB port, modem, Ethernet and other serial communication ports.

2.2 Device Functionality

This PED device support PIN entry, MAC calculation, cryptographic encryption/decryption related
EMV chip card, contactless EMV chip and Magnetic stripe card transaction
This machine provides a complete portfolio of connectivity to USB host/device, Ethernet, Modem and Serial port

2,3 Device Identification

Please refer below photo for IC3500 appearance.
The model name is printed top right side of LCD display and Hardware version in the label attached to bottom of case.

This device should be used according to the original purpose. (security EFT-POS) We do not allowed any other purpose used.

2.4 Version information

- The device hardware version is printed on label at bottom of case
- Software version is shown on the bottom area of LCD display during device start up.

User should check software and firmware version of device at field.
Please follow up below operation to see device firmware information

- After boot up, please push setup button on screen.
- Please press “2”,”5”,”8”,”0” and “confirm” button

2.5 General Instructions

- There is no security default value that needs to be updated by the end user.
- No authentication is required to use device after receiving by the end user.
- If there are any updates or patches can be loaded into device, they are cryptographically authenticated by the device. If the authenticity is failed, the updates or patch loading is rejected.

2.6 Software Development Guidance

IC3500 firmware/application implements the required security measures with functions to compliant PCI security requirements for authenticated applications.

2.1 2.7 Software update and patch procedure

The Bitel terminal will only accept offline update and patch, If the update and Patch in field can be allowed authentication Custom service and certificated agency only. Do not change any other App or Non authentication person. The SW loading process does not need to be protected in any special way other than installation best practices. Since the device will refuse to load any unauthenticated SW. The software can be updated using a specific command documents and application by the Bitel supports. If you can find terminal was not currently last version. Please contact Certified A/S or Bitel agency.

3. Installation Guidance

3.1 Roles.

User should refer user manual before installation this device.

The device consist of following items

- Device
- Power cable and connector
- User manual

All software is installed before deliver to end user. So, user can use Pin entry normally.

3.2 Visual Shielding

This device’s approval is subject to the implementation of visual deterrence by end-users of the device. In order to meet PCI requirements, measures must be implemented during device installation that limit viewing angles during PIN entry either through privacy shield or installation environment. Failure to implement these measures will invalidate the approval of this device.

“For more information on privacy shield minimum specifications or installed environment criteria, please refer to PCI PTS DTR’s v4, Appendix A.”

4. Device Security

4.1 Environmental Requirements

This device is targeting to use in attended environment and the security of the device is not compromising By altering the environment condition such as temperature, operating voltage outside and etc.

4.1.1 Temperature Environments

Operation Temperature : 0 ℃ ~ 50℃
Storage Temperature : -15℃ ~ 60℃

- If your Environment status is over that range, the terminal is not always working.
- If you can see warning message “Temper detect Contact A/S”. Please contact Bitel Agency or authorized service agent.)

4.1.2 Power Environments

Input :AC 100 ~ 240V 50/60Hz, 1.1A
Output : 24V (DC) 2.1A

- Only a Bitel approved Power Supply (CE Marked) specified for use with this terminal may be used.
- Do not allowed other external power supply and power source.
- Please follow the user manual for details related to all of the power system.

4.2 Hardware Security

The device contains tamper mechanism. In the event of tamper detection, the device will enter disable state, Touchscreen is locked and warning message display in screen “ Tamper detection Contact A/S Center” The device make the out of service If the device is locked, Please contact your technical Service partner or contact directly to Bitel Agency.

4.3 Software Security

The device is performed self- test upon start up. Also, the self-test is scheduled to run within 24 hours after start up. During self-test, the device perform integrity and authenticity of the software with checking hardware security status. If the self-test fail, the device goes in out of service and handles same as hardware tamper attack.

4.4 Privacy Shield & Terminal Installation

The following techniques can be employed to provide for effective screening of the PIN-entry keypad during the PIN entry process. These methods would typically be used in combination, though in some cases a method might be used singly.

- Positioning of terminal on the check-stand in such way as to make visual observation of the PIN-ent ry process infeasible. Examples include:
  - Visual shields designed into the check-stand. The shields may be solely for shielding purposes, or may be part of the general check-stand design.
  - Position the PED so that it is angled in such a way to make PIN spying difficult.
  - Installing PED on an adjustable stand that allows consumers to swivel the terminal sideways

and/or tilt it forwards/backwards to a position that makes visual observation of the PIN-entry process difficult.

- Positioning of in-store security cameras such that the PIN-entry keypad is not visible.
- Also recommends Instruction of the cardholder regarding safe PIN-entry. This can be done with a combination of
  - Signage on the PED
  - Prompts on the display, possibly with a “click-through” screen
  - Potentially literature at the point of sale
  - A logo for safe PIN-entry process

- The following table describes the preferred mounting methods and the recommended measure to protect from PIN capture in four observation corridors:

Method	Cashier	Customer In Queue	Customers Elsewhere	On-Site Cameras
Countertop without stand	Use signage behind the PED	Install so that customer is between PED and next in queue	No action needed	Do not install within view of cameras

4.5. ICC slot

Before using Chip card for ICCR, You must check the device status daily inspection in light environment or using light source. Please double check below method.

- First check outside enclose, It is the right product. No modified, No damage, No evidence cutting and adhesive.
- Check no evidence of unusual wires that has been connected to ICCR inside.
- There is no shim device in the slot of ICC acceptor
- There no resistance or loosing when inserting the card.
- Inserted Card direction is to parallel in LCD vertical direction.(Please refer to user manual picture)
-When the card is inserted into the exposed portion of the card in the direction of half size.

Such checks would provide warning of any unauthorized modifications to or substitution of the terminal, or suspicious behavior of individuals that have access to the terminal

5. Key Management

5.1 Key Management System

The device support different types of key management techniques as follows.

Fixed key: unique key for each terminal
Master/Session key: hierarchy of keys
DUKPT: Unique key for each transaction

5.2 Cryptographic Algorithms

The device implements following algorithms.

AES (128 bits)
RSA (Signature verification, 2048 bits)
SHA-256(Signature digest)
TDES (112 and 168bits)

5.3 Key table

Key name	Purpose	Algorithm	Size	storage
KBPK	Enciphering the key block when loading all keys	TDES	128	Secure area
Master Key	Decryption of session keys(PEK, MAC)	TDES	128 or 64	Secure area
MAC key	Message authentication	TDES	128 or 64	Secure area
PIN Key	Online PIN encryption key	TDES	128 or 64	Secure area
DUKPT Key	Online PIN encryption key	TDES	128 or 64	Secure area
CAPK	Authentication of issuer key from IC card	RSA	varies	Secure area
CAPK	Authentication of firmware	RSA	2048	Secure area
Auth key	Authentication on keys for financial transaction	RSA	2048	Secure area
AES key	Secure storage memory encryption	AES	128	Secure area

Cryptographic keys must be used only for their sole intended purpose.
For example, a cryptographic key used for PIN encryption must not be used for message authentication.
A PIN key must only ever be used for PIN encryption.

5.4 Key loading policy

The device doesn't accept manual cryptographies key entry. The device requested authentication by Key loading tools which meet key management requirement.
The keys are managed under split knowledge and dual control by ensuring that multiple personnel are required to undertake specific actions and respond to requests regarding effective key management procedures.

KBPK initially loaded in plaintext on device.
All other keys then loaded under symmetric key. (KBPK)
Keys used for PIN/MAC functions are loaded as session keys on device, encrypted by a previous loaded acquirer master key.

5.5 Key Removal

If tamper event is detected, all the keys in the device will be erased automatically.
After the keys are loaded to device, they will be available until administrator wants to erase all keys for decommissioning or tampering detected.

If the compromise of the original key Is known or suspected, user can still use another working keys still safely. But, It is requested to send the device to authorized service center for removal or re-download new keys.

6. System Administration

- The device is functional without any sensitive value setting when received by merchant. So, no sensitive security configuration setting is required to use device for user.

- Sensitive data inside device have to delete before refurbishing or remove device from service.
  If device goes to tamper status, all sensitive data inside device will be erased automatically.
  Please disassemble device to go tampering status.

- changing of default passwords
Password change process is enforced during first boot of device.
The sensitive service can not be accessed without finishing this process. if you want to change default password please refer to user manual.

- Open protocol
In current version of the device all open protocols modules and Ethernet interface have been disabled in firmware. Software guidance for open protocols will be added in future release of security policy document.

